Verification and Validation of Autonomous Systems

Charles Pecheur

Ames researchers, in collaboration with Carnegie Mellon University (CMU), are developing technologies for rigorously verifying requirements for software models used in autonomous controllers for space devices. These models describe the different components and failure modes of a complex device such as a spacecraft. They are used by the Livingstone fault recovery system to detect, diagnose, and recover from failures by comparing the observed condition of the spacecraft with the one predicted by the model.

Ames and CMU software scientists have developed a translation program that converts Livingstone models to the input language of SMV (Symbolic Model Verifier), a powerful verification tool based on symbolic model checking. The Livingstone-to-SMV translator is currently being used at Kennedy Space Center by engineers developing a Livingstone controller for the In-Situ Propellant Production (ISPP) system, a chemical processing device that will produce spacecraft fuel using the carbon dioxide found in the atmosphere of Mars. They annotate the Livingstone model with formally expressed requirements, using general logic notation or predefined templates. A requirement can state, for example, that the system can reconfigure itself when a valve is stuck. As shown in figure 1, the model and requirements are translated and fed into SMV, which searches all possible situations allowed by the model for violations of the requirement. When a violation is found, SMV provides a counter-example scenario that is crucial for diagnosing the source of the problem. These counter-examples are translated back in terms of the original Livingstone model.

The Livingstone-to-SMV translator has also been used for other Livingstone applications, such as the Remote Agent autonomous spacecraft controller, and different robot controllers at CMU. The use of formal verification allows developers of Livingstone applications at Kennedy Space Center and elsewhere to better understand and improve the quality of their Livingstone models. As the number of components grows, the number of possible fault scenarios increases exponentially; for example, the current model of ISPP has about 10^{50} possible states. Although a case-by-case test suite can cover only a tiny fraction of these states, the symbolic technique used in SMV has the power to exhaustively consider the whole space, thus giving very reliable answers. The translator completely shields the Livingstone users from the technicalities of SMV, giving them the benefits of formal verification within their familiar Livingstone environment.

Point of Contact: C. Pecheur
(650) 604-3588
pecheur@ptolemy.arc.nasa.gov

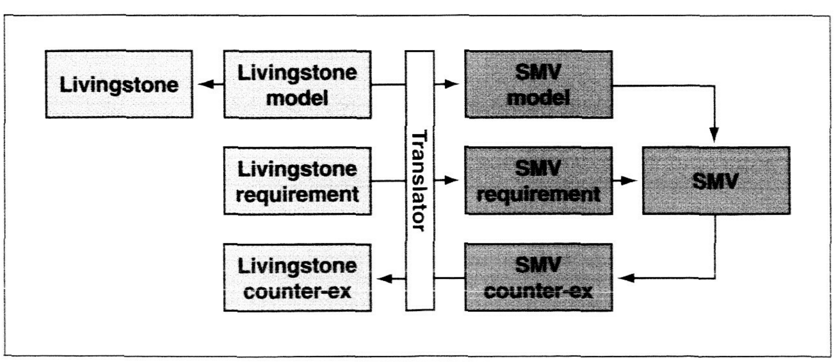

Fig. 1. Sitting in between the Livingstone fault recovery system and the SMV symbolic model checker, the translator developed at Ames and CMU provides Livingstone application developers with the powerful verification capabilities of SMV, while shielding them from the technicalities of the SMV tool.